Europ. J. Combinatorics (1994) **15**, 383–397

A Characterization of Certain Families of 4-Valent Symmetric Graphs

A. GARDINER AND CHERYL E. PRAEGER

Let Γ be a connected, 4-valent, G-symmetric graph. Each normal subgroup N of G gives rise to a natural symmetric quotient Γ_N, the vertices of which are the N-orbits on $V\Gamma$. If this quotient Γ_N is not itself 4-valent, then it was shown in [1] that either (i) N has at most two orbits on vertices of Γ, or (ii) N has $r \geqslant 3$ orbits on vertices and the quotient Γ_N is a circuit of length r. In the case in which N is elementary abelian, the graphs which can occur in (i) were classified in [1]. This paper classifies the most symmetrical graphs which can occur in (ii). We show that if N is a minimal normal elementary abelian p-subgroup of G and Γ_N is a circuit, then if $p = 2$, $\Gamma = C(2; r, s)$, and if p is odd then provided that the stabilizer of a vertex is as large as it can possibly be, Γ must be one of the graphs $C(p; r, s)$, $C^{\pm 1}(p; st, s)$ or $C^{\pm \varepsilon}(p; 2st, s)$ (Theorem 1.1). We also obtain a complete classification in the non-extremal case when p is odd and $|N| \leqslant p^2$. For all other cases we obtain much detailed information about Γ and G, but this does not appear sufficient to allow a general classification of possible pairs (Γ, G).

1. INTRODUCTION

In [1, Theorem 2.1] we showed that whenever Γ is a connected, G-symmetric, 4-valent graph and N is a normal subgroup of G, then one of the following holds:
(a) the quotient Γ_N is connected, G/N-symmetric, and has itself valency 4;
(b) N has just one or two orbits on $V\Gamma$;
(c) N has $r \geqslant 3$ orbits and the quotient Γ_N is a circuit C_r.
If we wish to classify some family of symmetric, 4-valent graphs, the first case (a) gives rise to a natural reduction. One would therefore like detailed information about the graphs which can arise in cases (b) and (c). Let N be an elementary abelian p-group. The graphs which can arise in case (b) were then classified in [1]; this paper contains a detailed study of the graphs which can arise in case (c). Our classification is complete only (i) when $p = 2$, or (ii) when p is odd and either $|N| \leqslant p^2$, or each vertex stabilizer is as large as it can possibly be. We prove the following:

THEOREM 1.1. *Let Γ be a connected, G-symmetric, 4-valent graph, and let N be a minimal normal p-subgroup of G with orbits of size p^s for some prime p. Let K denote the kernel of the action of G on N-orbits. Suppose that the quotient $\Gamma_N = C_r$ is a circuit of length $r \geqslant 3$. Then $s \leqslant r$ and one of the following holds*:
(a) $p = 2$, $C_K(N)$ does not act semi-regularly on $V\Gamma$, and $\Gamma = C(2; r, s)$.
(b) p is odd, $C_K(N)$ acts semi-regularly on $V\Gamma$, and the stabilizer $K(\alpha)$ of a vertex α is a non-trivial elementary abelian 2-group of order dividing 2^s. In the extremal case in which $|K(\alpha)| = 2^s$, we have $\Gamma = C^{\pm 1}(p; st, s)$ or $\Gamma = C^{\pm \varepsilon}(p; 2st, s)$ for some $t \geqslant 1$.

We note that when p is odd and $s = 1$, the additional hypothesis on $|K(\alpha)|$ is automatically satisfied. When $s = 2$ and $|K(\alpha)| = 2^s$, then Theorem 1.1(b) shows that $\Gamma = C^{\pm 1}(p; st, s)$ or $\Gamma = C^{\pm \varepsilon}(p; 2st, s)$; in Section 8 we look in detail at the other possibility when $s = 2$, namely $K(\alpha) = Z_2$. We prove the following:

THEOREM 1.2. *Let Γ be a connected, G-symmetric, 4-valent graph, and let $N = (Z_p)^2$, p an odd prime, be a minimal normal subgroup of G with orbits of size p^s. Let K denote the kernel of the action of G on N-orbits. If the quotient $\Gamma_N = C_r$ is a*

0195-6698/94/040383 + 15 $08.00/0

circuit of length $r \geq 3$, then one of the following holds:
(a) $s = 1$ or 2, $K(\alpha) = (Z_2)^s$, and $\Gamma = C^{\pm 1}(p; st, s)$ or $\Gamma = C^{\pm \varepsilon}(p; 2st, s)$ for some $t \geq 1$.
(b) $s = 2$, $K(\alpha) = Z_2$ and $\Gamma = C^{\pm 1}(p; 2t, 2)$, or Γ belongs to one of two families described in detail in Lemmas 8.4 and 8.7.

The families of graphs $C(p; r, s)$, $C^{\pm 1}(p; sr, s)$ and $C^{\pm \varepsilon}(p; 2st, s)$ are introduced in Section 2; see [1] for any other unexplained notation. In Section 3 we reduce to the case in which p is odd, and prove the basic facts about N-orbits, about N and about K. Section 4 looks at the action of the dihedral group G/K on N, introduces the 'distance 2' graph on each N-orbit, and uses these ideas to resolve the simplest case in which $N = Z_p$. Section 5 shows that the graphs in Theorem 1.1(b) all have an interesting G-symmetric quotient $\Gamma_p = C(p; r, s)$ of valency $2p$. In Section 6 we begin to pin down precisely how N acts on the graph and how $K(\alpha)$ acts on N in general. Section 7 concentrates on the extremal case $|K(\alpha)| = 2^s$, thus completing the proof of Theorem 1.1. In Section 8 we examine the easiest non-extremal case $|K(\alpha)| < 2^s$, namely when $s = 2$ and $K(\alpha) = Z_2$, and we prove a more precise version of Theorem 1.2.

2. Three Families of Graphs

The first of our three families was introduced in [2]. However, the definition given there seems designed to obscure the natural, and very general, idea common to all three of the families which occur in Theorem 1.1.

Definition 2.1: the graphs $C(p; r, s)$ of valency $2p$. Before giving the formal definition, we indicate where it comes from. We start with a circuit C_r and form the natural 'wreath product' $\bar{K}_p \operatorname{wr} C_r$ of a set $\bar{K}_p$ of p independent vertices by the circuit C_r: that is, we use the circuit C_r as a base space (or quotient); we then lift each vertex of C_r to a 'fibre' of p independent vertices and lift each edge of C_r to a complete bipartite graph $K_{p,p}$ joining the corresponding fibres. (This graph is sometimes called a 'lexicographic product' and is denoted by $C_r[\bar{K}_p]$.) Thus vertices of $\bar{K}_p \operatorname{wr} C_r$ are labelled by $Z_p \times Z_r$, where the vertex labelled (x, i), which we shall write as $(x)_i$ with $i \in Z_r$ as a subscript, is adjacent to $(y)_{i+1}$ for every $y \in Z_p$. The vertices of $C(p; r, s)$ are then the subgraphs of $\bar{K} \operatorname{wr} C_r$ corresponding to the 'clockwise' $(s-1)$-arcs; that is, the s-tuples $((x)_i, (y)_{i+1}, \ldots, (z)_{i+s-1})$. Two such $(s-1)$-arcs are adjacent in $C(p; r, s)$ precisely when they overlap in a common $(s-2)$-arc. All that is needed to specify such a (clockwise) $(s-1)$-arc is the initial subscript $i \in Z_r$ and the s-tuple $(x, y, \ldots, z) \in (Z_p)^s$. This should help to make sense of the formal definition below.

Before giving this formal definition, we consider automorphisms. The graph $\Delta = \bar{K}_p \operatorname{wr} C_r$ admits the group $H = S_p \operatorname{wr} D_{2r}$, where the ith direct factor S_p in the base group $(S_p)^r$ acts only on those vertices of Δ the label x_i of which has the fixed subscript $i \in Z_r$. This same group acts on clockwise $(s-1)$-arcs in Δ; that is, on the vertices of $C(p; r, s)$: the ith direct factor of the base group $(S_p)^r$ acts on the co-ordinate with subscript i, if it occurs, in the label $((x)_j, (y)_{j+1}, \ldots, (z)_{j+s-1})$. The dihedral group D_{2r} permutes the fibres in Δ and so acts on $(s-1)$-arcs in Δ (some elements will turn a clockwise $(s-1)$-arc into an anticlockwise $(s-1)$-arc, but this anticlockwise $(s-1)$-arc should be reinterpreted as its 'opposite' (clockwise) $(s-1)$-arc). Hence the same group $H = S_p \operatorname{wr} D_{2r}$ acts on the graph $C(p; r, s)$.

Formally, we define the graph $\Gamma = C(p; r, s)$ to have vertex set $(Z_p)^s \times Z_r$, where each vertex $(x_1, x_2, \ldots, x_s)_i$, with $x_1, x_2, \ldots, x_s \in Z_p$, and $i \in Z_r$ is adjacent to

$(x_2, \ldots, x_s, x_{s+1})_{i+1}$, for every $x_{s+1} \in Z_p$. (We note that the vertex $(y_1, y_2, \ldots, y_s, i)$ in [2] corresponds to that labelled $(y_{s-1}, y_{s-3}, \ldots, y_{s-4}, y_{s-2}, y_s)_i$ here.)

The graph $\Gamma = C(p; r, s)$ is H-symmetric provided that $r > s$. Moreover, it was shown in [2, Theorem 1.13] that H is the full group of automorphism unless (a) $(r, s) = (4, 1)$, $C(p; 4, 1) = K_{2p,2p}$, or (b) $(p, r, s) = (2, 4, 2)$, $C(2; 4, 2) = H_{4,2} = Q_4$, or (c) $(p, r, s) = (2, 4, 3)$. The subgroup $G = Z_p \operatorname{wr} D_{2r}$ also acts symmetrically on Γ when $r > s$. Moreover, G has a normal, elementary abelian subgroup $C = (Z_p)^r$ which has orbits of size p^s on vertices of Γ. These orbits form a G-invariant partition $\mathbf{B}$ of $V\Gamma$ with quotient $\Gamma_C = C_r$.

Definition 2.2: the graphs $C^{\pm 1}(p; st, s)$ of valency 4. The graph $\Gamma = C^{\pm 1}(p; st, s)$ has vertex set $(Z_p)^s \times Z_{st}$. Each vertex $(x_0, x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_{s-1})_{ms+i}$ $(0 \leq m < t)$ is adjacent to just two vertices with subscript $ms + i + 1$, namely $(x_0, x_1, \ldots, x_{i-1}, x_i \pm 1, x_{i+1}, \ldots, x_{s-1})_{ms+i+1}$.

The group $N = \langle a(0) \rangle \times \langle a(1) \rangle \times \cdots \times \langle a(s-1) \rangle = (Z_p)^s$ acts on $V\Gamma$ in the natural way, inducing translations on the first s co-ordinates and leaving the subscript (in Z_{st}) unchanged: thus $a(j)^k$ adds k to the jth co-ordinate x_j. Γ also admits automorphisms σ, $w(0)$ and τ, where for each $q \in Z_{st}$ and $x_0, \ldots, x_{s-1} \in Z_p$ we have

$$(x_0, x_1, \ldots, x_{s-2}, x_{s-1})_q^\sigma = (x_{s-1}, x_0, \ldots, x_{s-2})_{q+1},$$

$$(x_0, x_1, \ldots, x_{s-1})_q^{w(0)} = (-x_0, x_1, \ldots, x_{s-1})_q,$$

$$(x_0, x_1, \ldots, x_{s-2}, x_{s-1})_q^\tau = (x_{s-1}, x_{s-2}, \ldots, x_1, x_0)_{s-q}.$$

Let $G = \langle N, w(0), \tau, \sigma \rangle$. Then Γ is G-symmetric and $N \lhd G$. If Δ_i denotes the set of all vertices with fixed subscript $i \in Z_{st}$, then N acts regularly on each Δ_i, so $\mathbf{B} = \{\Delta_0, \Delta_1, \ldots, \Delta_{st-1}\}$ is a G-partition of $V\Gamma$ with quotient $\Gamma_N = C_{st}$. If $w(i) = w(0)^{\sigma^i}$, then $\langle w(0), w(1), \ldots, w(s-1) \rangle = (Z_2)^s$ fixes each vertex $\mathbf{0}_i = (0, \ldots, 0)_i$ $(i \in Z_{st})$ and $K = N \cdot \langle w(0), w(1), \ldots, w(s-1) \rangle$ is the kernel of the action of G on $\mathbf{B}$.

There is an alternative definition of the graphs $C^{\pm 1}(p; r, s)$, whic emphasizes the connections with the previous family $C(p; r, s)$, but for which the action of N is more confusing. We use the same labelling set $(Z_p)^s \times Z_{st}$, but cycle the co-ordinates in a similar way to Definition 2.1: thus $(x_0, x_1, \ldots, x_{s-1})_i$ is adjacent to $(x_1, \ldots, x_{s-1}, x_0 \pm 1)_{i+1}$. Each basis element $a(j)$ in the group $N = \langle a(0) \rangle \times \cdots \times \langle a(s-1) \rangle = (Z_p)^s$ now has to act on the 'appropriate' co-ordinate of $(x_0, x_1, \ldots, x_{s-1})_i$; namely, $a(j)$ acts on the kth co-ordinate, changing x_k to $x_k + 1$, where $k \equiv j - i \pmod s$, and leaves all other co-ordinates unchanged. We shall use this representation.

Definition 2.3: the graphs $C^{\pm\varepsilon}(p; 2st, s)$ of valency 4. The definition is just like that for the graph $C^{\pm 1}(p; st, s)$, but with one extra complication. Let p be a prime, $p \equiv 1 \pmod 4$, and let ε be a square root of $-1 \pmod p$. The graph $\Gamma = C^{\pm\varepsilon}(p; 2st, s)$ has vertex set $(Z_p)^s \times Z_{2st}$. Each vertex $(x_0, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_{s-1})_{ms+i}$ is adjacent to $(x_0, \ldots, x_{i-1}, x_i \pm u, x_{i+1}, \ldots, x_{s-1})_{ms+i+1}$, where $u = 1$ if m is even and $u = \varepsilon$ if m is odd.

The group $N = \langle a(0) \rangle \times \langle a(1) \rangle \times \cdots \times \langle a(s-1) \rangle = (Z_p)^s$ acts in the obvious way on the first s co-ordinates and leaves the subscript (in Z_{2st}) unchanged: thus $a(j)^k$ adds k to the jth co-ordinate x_j. Γ also admits automorphisms σ, $w(0)$ and τ, where

$$(x_0, \ldots, x_{s-2}, x_{s-1})_q^\sigma = (\varepsilon x_{s-1}, x_0, \ldots, x_{s-2})_{q+1},$$

$$(x_0, x_1, \ldots, x_{s-1})_q^{w(0)} = (-x_0, x_1, \ldots, x_{s-1})_q,$$

$$(x_0, x_1, \ldots, x_{s-2}, x_{s-1})_q^\tau = (x_{s-1}, x_{s-2}, \ldots, x_1, x_0)_{s-q}.$$

Let $G = \langle N, w(0), \tau, \sigma\rangle$. Then Γ is G-symmetric and $N \lhd G$. If Δ_i denotes the set of all vertices with fixed subscript $i \in Z_{2st}$, then N acts regularly on each Δ_i, so $\mathbf{B} = \{\Delta_0, \Delta_1, \ldots, \Delta_{2st-1}\}$ is a G-partition of $V\Gamma$ with quotient $\Gamma_{\mathbf{B}} = C_{2st}$. If $w(i) = w(0)^{\sigma^i}$, then $\langle w(0), w(1), \ldots, w(s-1)\rangle = (Z_2)^s$ fixes each vertex $\mathbf{0}_i$ $(i \in Z_{2st})$ and $K = N \cdot \langle w(0), w(1), \ldots, w(s-1)\rangle$ is the kernel of the action of G on $\mathbf{B}$.

As in Definition 2.2, there is an alternative formulation which brings out the links with Definition 2.1, but which makes the action of N on vertices harder to work with. In this alternative definition $(x_0, x_1, \ldots, x_{s-1})_i$ is adjacent to $(x_1, \ldots, x_{s-1}, x_0 \pm u)_{i+1}$ where $u = \varepsilon$ if $\lfloor i/s \rfloor$ is even and $u = 1$ if $\lfloor i/s \rfloor$ is odd. The basis element $a(j)$ in $N = \langle a(0)\rangle \times \cdots \times \langle a(s-1)\rangle$ now acts on the kth co-ordinate of $(x_0, x_1, \ldots, x_{s-1})_i$, changing x_k to $x_k + 1$, where $k \equiv j - i \pmod s$, and leaves all other co-ordinates unchanged. We shall not use this representation.

3. A First Look at N-orbits

Throughout the rest of this paper Γ denotes a connected, 4-valent, G-symmetric graph, and N is a minimal normal elementary abelian p-subgroup of G having $r \geq 3$ orbits on vertices and quotient $\Gamma_N = C_r$. We denote the N-orbits by $\Delta_0, \Delta_1, \ldots, \Delta_{r-1}$, labelled cyclically so that each Δ_i $(0 \leq i < r)$ is adjacent to Δ_{i+1} in the quotient $\Gamma_N = C_r$. The subgroup K which leaves each Δ_i invariant clearly contains N.

Lemma 3.1. (a) *The vertex stabilizer $G(\alpha)$ of α in G is a 2-group. $G(\alpha)^{\Gamma(\alpha)}$ is transitive, $K(\alpha)$ is a non-trivial subgroup of index 2 in $G(\alpha)$, and $K = N \cdot K(\alpha)$. The group $C = C_K(N)$ is abelian.*

(b) *If C does not act semi-regularly on vertices, then $\Gamma = C(2; r, s)$, where $r > s \geq 1$ and $r \geq 3$.*

(c) *If C does not act semi-regularly on vertices, then $C = N = (Z_p)^s$ for some odd prime p and some $s \geq 1$. Moreover, $K(\alpha)$ fixes one vertex α_i in each Δ_i $(0 \leq i \leq r-1)$. Each set Δ_i may be identified with N in such a way that N acts on each Δ_i by right multiplication and $K(\alpha) = K(\alpha_i)$ acts on Δ_i by conjugation.*

Proof. (a) The subsets $\Gamma(\alpha) \cap \Delta_{r-1}$ and $\Gamma(\alpha) \cap \Delta_1$ of $\Gamma(\alpha)$ form a block system for $G(\alpha)^{\Gamma(\alpha)}$. Hence $G(\alpha)^{\Gamma(\alpha)}$ is a transitive subgroup of D_8, so $G(\alpha)$ is a 2-group. Since $G/K = D_{2r}$, $K(\alpha)$ has index 2 in $G(\alpha)$. Hence $K(\alpha)^{\Gamma(\alpha)} \neq 1$ (since $|G(\alpha)^{\Gamma(\alpha)}| \geq 4$), so $K(\alpha) \neq 1$.

Clearly, $C = C_K(N) \geq N$. Since N is abelian and K leaves each N-orbit Δ_i invariant, we must have $C^{\Delta_i} = N^{\Delta_i}$ for each i. Hence the commutator subgroup $[C, C]$ fixes each Δ_i pointwise, so C is abelian.

(b) If C is not semi-regular on vertices, then $\Gamma = C(2; r, s)$ by [2, Theorem 2.1].

(c) Suppose that C acts semi-regularly on vertices. Then $C = N$. Since $K(\alpha) \neq 1$, we have $K = N \cdot K(\alpha) > N$. If N is a 2-group, then so is K; hence $Z(K) \cap N \neq 1$. Since $C_{K(\alpha)}(N) = 1$, we have $1 \neq Z(K) < N$, contradicting the minimality of N. Thus we must have $N = (Z_p)^s$ for some *odd* prime p.

Since $K = N \cdot K(\alpha)$, N has a unique conjugacy class of complements in K, namely the Sylow 2-subgroups of K. It follows that $K(\alpha)$ fixes at least one vertex α_i in Δ_i for each i. Since N acts semi-regularly on $V\Gamma$, we can identify each vertex $\beta \in \Delta_i$ with the unique element n in N such that $\beta = \alpha_i^n$. Then N acts by right multiplication on each Δ_i, and $K(\alpha) = K(\alpha_i)$ acts by conjugation on each Δ_i. It follows that $K(\alpha)$ fixes *precisely one* point α_i in Δ_i for each i; (otherwise, $K(\alpha)$ would centralize some non-identity element in N, so we would have $1 \neq C_N(K(\alpha)) = Z(K) \cap N \lhd G$; the minimality of N would then force $N \leq Z(K)$, so $C = C_K(N) = K$ and $K = N$, which is not the case). $\square$

From now on we shall assume that we are in the situation covered by case (c) *in Lemma* 3.1: *i.e. C acts semi-regularly, and* $C = N = (Z_p)^s$ *for some odd prime p.*

In identifying the vertices in Δ_i with elements of N, we shall denote the vertex $\alpha_i^n \in \Delta_i$ by n_i. In Lemma 3.1(c) we observed that $K(\alpha)$ acts on these labels by conjugation. We shall need the following more general fact.

LEMMA 3.2. *Suppose that* $g \in N_G(K(\alpha))$ *maps* Δ_i *to* Δ_j. *If* $\beta = \alpha_i^n = n_i \in \Delta_i$, *then* $\beta^g = (n^g)_j$; *that is, g acts on labels in N by conjugation.*

PROOF. $\beta^g = (\alpha_i^n)^g = (\alpha_i^g)^{n^g} = (\alpha_j)^{n^g} = (n^g)_j$. □

Our whole approach to the problem of identifying the graph Γ has its roots in the following elementary observation.

LEMMA 3.3. *For each* $i \in Z_r$, *the subgraph of* Γ *induced on* $\Delta_i \cup \Delta_{i+1}$ *is a union of* p^{s-1} *disjoint cycles, each of length 2p. The distinguished 'base points'* α_i *and* α_{i+1} *belong to the same cycle, namely*

$$(\alpha_i = 1_i, a_{i+1}, a_i^2, a_{i+1}^3, a_i^4, \ldots, a_{i+1}^p = 1_{i+1} = \alpha_{i+1}, a_i, a_{i+1}^2, \ldots, a_i^{-2}, a_{i+1}^{-1}, 1_i = \alpha_i),$$

for some $a \in N - \{1\}$.

PROOF. Let $\Gamma(\alpha_i) \cap \Delta_{i+1} = \{a_{i+1}, b_{i+1}\}$. Then a and b are distinct elements of N, neither of which is the identity (since $K(\alpha)$ conjugates one to the other). We show that $b = a^{-1}$.

Since $\alpha_i = 1_i$ is joined to a_{i+1} and b_{i+1}, and since N acts on $\Delta_i \cup \Delta_{i+1}$ by right multiplication we have $\Gamma(\alpha_{i+1}) \cap \Delta_i = \{a_i^{-1}, b_i^{-1}\}$. The subgraph induced on $\Delta_i \cup \Delta_{i+1}$ is regular of valency 2, and the setwise stabilizer of $\Delta_i \cup \Delta_{i+1}$ in G acts transitively on ordered edges and thus on components. Hence this subgraph is the union of q disjoint cycles, each of length $2t$, for some q and t. We can use the action of the subgroup $\langle a, b\rangle$ of N to write down the whole cycle γ containing α_i:

$$\gamma = (b_{i+1}, \alpha_i = 1_i, a_{i+1}, (b^{-1}a)_i, (b^{-1}a^2)_{i+1}, (b^{-2}a^2)_i, (b^{-2}a^3)_{i+1}, \ldots).$$

Since $b^{-1}a$ has order p, it follows that the cycle has length $2p$; so $t = p$ and $q = p^{s-1}$. Moreover, $K(\alpha_i)$ contains an element τ fixing α_i and interchanging a_{i+1} and b_{i+1}. This element τ induces a reflection of the cycle γ and so fixes only α_i and the vertex opposite α_i on γ. Hence every element of $K(\alpha_i)$ fixes the vertex opposite α_i on γ, so this vertex must be $\alpha_{i+1} = 1_{i+1}$. Hence $1_{i+1} = (b^{-j}a^{j+1})_{i+1}$, where $j = (p-1)/2$; that is, $b^{(p-1)/2} = a^{(p+1)/2} \in \langle a\rangle$. Hence $b = a^{-1}$. □

Note that the element a depends on i; to stress this we denote it by $a(i)$.

4. THE GENERAL PICTURE AND THE EASIEST CASE

Since G/K induces the dihedral group D_{2r} on $\Gamma_N = C_r$, G must contain elements σ and τ, where σ induces a rotation of the circuit C_r and τ induces a reflection. Thus we may choose σ to map each Δ_i to Δ_{i+1} $(i \in Z_r)$, and we may choose τ to interchange each Δ_i with Δ_{s-i} $(i \in Z_r)$.

Since Γ is G-symmetric, we may choose σ to map the 1-arc $(\alpha_0, \alpha_1^{a(0)})$ to the 1-arc $(\alpha_1, \alpha_2^{a(1)})$. Hence σ normalizes $K(\alpha_0) = K(\alpha_1)$; thus, by Lemma 3.2, σ conjugates $a(0)$ to $a(1)$. Since σ normalizes $K(\alpha_0)$, it must map α_i to α_{i+1} for each $i \in Z_r$, and so conjugates each $a(i)$ either to $a(i+1)$ or to $a(i+1)^{-1}$. Now for each $i \in Z_r$, it is only the *pair* $\{a(i), a(i)^{-1}\}$ that is determined by Lemma 3.3; thus we may choose each $a(i+1)$ so that $a(i)^\sigma = a(i+1)$ for each $i = 0, 1, \ldots, r-2$. Then $a(r-1)^\sigma \in \{a(0), a(0)^{-1}\}$.

Similarly, we may choose τ to map the 1-arc $(\alpha_0, \alpha_1^{a(0)})$ to the 1-arc $(\alpha_s, \alpha_{s-1}^{a(s-1)})$. Then τ also normalizes $K(\alpha_0) = K(\alpha_s)$ and so conjugates $a(0)$ to $a(s-1)$. We have proved the following:

LEMMA 4.1. (a) *G contains an element σ which maps each distinguished vertex α_i to α_{i+1} ($i \in Z_r$), and which normalizes $K(\alpha_0)$. If $\Gamma(\alpha_i) \cap \Delta_{i+1} = \{a(i)_{i+1}, a(i)_{i+1}^{-1}\}$, then we can choose the elements $a(i)$ so that σ conjugates $a(i)$ to $a(i+1)$ for each $i < r-1$, and $a(r-1)^\sigma \in \{a(0), a(0)^{-1}\}$.*

(b) *G contains an element τ which interchanges α_0 and α_s, which normalizes $K(\alpha_0)$, and which conjugates $a(0)$ to $a(s-1)$.* □

The first key combinatorial idea is to observe that the circuits introduced in Lemma 3.3 guarantee that, for each α_i, there are just two vertices in Δ_i which are at distance 2 from α_i via a vertex of Δ_{i+1}, namely $a(i)_i^2$ and $a(i)_i^{-2}$. Similarly, there are just two vertices in Δ_i which are at distance 2 from α_i via a vertex of Δ_{i-1}, namely $a(i-1)_i^2$ and $a(i-1)_i^{-2}$. Thus Γ induces a graph Δ_i' on each N-orbit Δ_i, where two vertices in Δ_i are adjacent in Δ_i' whenever they are at distance 2 in Γ. The connected components of each Δ_i', $i = 0, 1, \ldots, r-1$, have valency 4 and form the equivalence classes of a G-invariant equivalence relation ρ on $V\Gamma$. (Note that since we may have $\{a(i-1), a(i-1)^{-1}\} = \{a(i), a(i)^{-1}\}$, we have to allow the possibility that each 4-valent component of Δ_i' may consist of the circuit C_p with all edges doubled.)

LEMMA 4.2. *The connected components of the distance 2 graph Δ_i' induced by Γ on each Δ_i define a G-invariant equivalence relation ρ. The subgroup of N which leaves each ρ-class in Δ_i invariant is precisely $N_i = \langle a(i-1), a(i)\rangle$, so each ρ-class has size* $|N_i| = p$ or p^2.

PROOF. If two vertices of Δ_i are at distance 2 in Γ via some vertex of Δ_{i+1}, their labels differ either by $a(i)^2$ or by $a(i)^{-2}$. If two vertices of Δ_i are at distance 2 in Γ via some vertex of Δ_{i-1}, their labels differ either by $a(i-1)^2$ or by $a(i-1)^{-2}$. Hence the connected components of the distance 2 graph Δ_i' induced on Δ_i are precisely those subsets of Δ_i labelled by cosets of the subgroup $\langle a(i-1)^2, a(i)^2\rangle = \langle a(i-1), a(i)\rangle = N_i$ in N. □

Note that since G acts transitively on 1-arcs of Γ, the group induced on each component of Δ_i' by its stabilizer in G must act transitively on 1-arcs of Δ_i'. Moreover, this stabilizer contains an elementary abelian normal subgroup N_i with just one orbit on that component. Hence we know from [1, Theorem 1.2] that each component is one of the following (and that all components are isomorphic):

(a) $C_p^{(2)}$, a circuit of length p with each edge doubled;

(b) a prime circulant $C(p; \pm 1, \pm\varepsilon)$, where $p \equiv 1 \pmod 4$ and ε is a square root of $-1 \pmod p$;

(c) a two-dimensional grid $G(p^2) = C_p \times C_p$.

Before concentrating on the generic case (c), we first resolve the cases in which $|N_i| = p$ (cases (a) and (b)). Without explicitly using the graphs Δ_i' we show (Theorem 4.3) that $|N_i| = p$ implies $N = N_i = Z_p$, so that each N-orbit contains a single ρ-class. We then classify the graphs which can occur.

THEOREM 4.3. *Suppose that* $|N_1| = p$; *that is,* $\langle a(0)\rangle = \langle a(1)\rangle$. *Then* $N = N_1 = Z_p$, $K(\alpha_0) = \langle w(0)\rangle = Z_2$ *and either*:
(i) $\sigma^\tau = \sigma^{-1}$ and $\Gamma = C^{\pm 1}(p; r, 1)$; *or*
(ii) $\sigma^\tau = w(0)\sigma^{-1}$, $p \equiv 1 \pmod 4$, *and* $\Gamma = C^{\pm\varepsilon}(p; 2t, 1)$.

PROOF. Suppose that $\langle a(0)\rangle = \langle a(1)\rangle$. Then $a(0)^\sigma = a(1) = a(0)^v$ for some v. Hence $N_1 = \langle a(0)\rangle$ is normalized by $\langle N, G(\alpha_0), \sigma\rangle = G$, so $N = N_1 = Z_p$ (by the minimality of N).

Since $s = 1$, the element τ in G maps the 1-arc $(\alpha_0, \alpha_1^{a(0)})$ to the 1-arc $(\alpha_1, \alpha_0^{a(0)})$, so τ interchanges α_0 and α_1 and centralizes $a(0)$ (Lemma 4.1(b)). Moreover, τ^2 fixes α_0, leaves each Δ_i $(i \in Z_r)$ invariant, and centralizes $N = \langle a(0)\rangle$, so $\tau^2 \in C_{K(\alpha_0)}(N) = 1$ (Lemma 3.1(c)). Hence $\tau^2 = 1$.

Similarly, the element $(\tau\sigma)^2$ fixes α_0 and α_1 and leaves each Δ_i invariant, so $(\tau\sigma)^2 \in K(\alpha_0)$. Thus $(\tau\sigma)^2$ must leave $\Gamma(\alpha_0) \cap \Delta_1 = \{\alpha_1^{a(0)}, \alpha_1^{a(0)^{-1}}\}$ invariant. But $(\tau\sigma)^2$ conjugates $a(0)$ to $a(0)^{v^2}$; hence $v^2 = \pm 1$. To identify the element $(\tau\sigma)^2$ observe that $K(\alpha_0)$ acts on N by conjugation and $C_{K(\alpha_0)}(N) = 1$ (Lemma 3.1(c)), so $K(\alpha_0) \leqslant \operatorname{Aut} N = Z_{p-1}$. Since $K(\alpha_0)$ leaves $\Gamma(\alpha_0) \cap \Delta_1$ invariant, $K(\alpha_0)$ can only invert $N = \langle a(0)\rangle$, so $K(\alpha_0) = \langle w(0)\rangle = Z_2$. Hence either (i) $v^2 = 1$, $(\tau\sigma)^2 = 1$ and $\sigma^\tau = \sigma^{-1}$, or (ii) $v^2 = -1$, $(\tau\sigma)^2 = w(0)$ and $\sigma^\tau = w(0)\sigma^{-1}$.

In case (i), $v = \pm 1$, so $\{a(0), a(0)^{-1}\} = \{a(1), a(1)^{-1}\}$. Conjugating by σ we see that $\{a(i), a(i)^{-1}\} = \{a(0), a(0)^{-1}\}$, for every $i \in Z_r$. If we write the group $N = Z_p$ additively with $a(0) = 1$ as the distinguished generator, and denote each vertex α_i^n by its label n_i, then vertices in Γ are labelled by $Z_p \times Z_r$, with each vertex the label of which has subscript $i \in Z_r$, say n_i, adjacent to the two vertices $(n \pm 1)_{i+1}$. Hence $\Gamma = C^{\pm 1}(p; r, 1)$.

In case (ii) we must have $p \equiv 1 \pmod 4$, and $v = \pm\varepsilon$ is then a primitive fourth root of $1 \pmod p$. Arguing as in the previous case, we see that $\{a(2i), a(2i)^{-1}\} = \{a(0), a(0)^{-1}\}$ and $\{a(2i+1), a(2i+1)^{-1}\} = \{a(1), a(1)^{-1}\} = \{a(0)^\varepsilon, a(0)^{-\varepsilon}\}$ for all $i \in Z_r$. Hence $r = 2t$ must be even and, labelling as in case (i), we see that $\Gamma = C^{\pm\varepsilon}(p; 2t, 1)$. □

5. THE QUOTIENT Γ_ρ

In the light of Theorem 4.3 we may assume from now on that the groups $N_i = \langle a(i-1), a(i)\rangle$ all have order p^2. In this section we show that the connected components of the graphs Δ_i' form the equivalence classes of a G-invariant equivalence relation ρ, the quotient Γ_ρ of which is precisely the graph $C(p; r, s-2)$ of valency $2p$ (see Definition 2.1). We also show how to match up the labelling of vertices in $C(p; r, s-2)$ with the most obvious properties of Γ.

These observations played a significant role in our original approach, and may be important in tacking the general case which we leave unresolved (where the stabilizer $K(\alpha)$ has order less than 2^s; see Theorem 1.1). The approach now adopted in Sections 6–8 is direct and only uses the ideas of this section in the proof of Lemmas 6.1 and 6.2(b).

As noted in the previous section, the connected components of the distance 2 graph Δ_i' induced on each Δ_i are 4-valent and $G(\Delta_i)$-symmetric, where $G(\Delta_i)$ has a regular elementary abelian normal subgroup N_i of order p^2. Thus by [1, Theorem 1.2] we have the following results.

LEMMA 5.1. *Each connected component of Δ_i' ($i \in Z_r$) has size p^2 and is isomorphic to a two-dimensional grid $G(p^2) = C_p \times C_p$.*

LEMMA 5.2. (a) *Δ_i' is connected precisely when $N = N_i = (Z_p)^2$. In this case $\Gamma_\rho = \Gamma_N = C_r$. (Note that interpreting this quotient C_r as $C(p; r, 0)$ brings this case into line with part* (b).)

(b) *If Δ_i' is not connected, then Γ_ρ has valency $2p$, G acts faithfully on Γ_ρ, and Γ_ρ is G-symmetric and is isomorphic to $C(p; r, s-2)$, $r \geq s$.*

PROOF OF LEMMA 5.2. (a) This is straightforward.

(b) Suppose that the distance 2 graph induced on Δ_i is not connected. For $\beta \in V\Gamma$, let $\rho(\beta)$ denote the ρ-class containing β. Thus $\rho(\alpha_0) = \{n_0 : n \in \langle a(r-1), a(0)\rangle\} = (N_0)_0$. The subset of vertices in Δ_1 adjacent to vertices of $\rho(\alpha_0)$ is precisely $(N_0)_1$ (since $\Gamma(\alpha_0) \cap \Delta_1 = \{a(0)_1, a(0)_1^{-1}\}$ and N_0 acts by right multiplication on both Δ_0 and Δ_1, and leaves $\rho(\alpha_0)$ invariant). If $(N_0)_1$ were a single ρ-class, then the quotient Γ_ρ would have valency 2 and so would be a cycle. But then N_0 would be normalized by $\langle N, G(\alpha_0), \sigma\rangle$, so we would have $N_0 = N$ (by the minimality of N), and we would be in case (a), contrary to assumption. Thus $(N_0)_1$ must contain vertices from more than one ρ-class. Since $\langle a(0)\rangle_1$ is contained in a single ρ-class, and since $N_0 = (Z_p)^2$ acts transitively on the set of ρ-classes involved in $(N_0)_1$, $(N_0)_1$ must contain p points from each of p different ρ-classes. It follows that the quotient Γ_ρ has valency $2p$ and is G-symmetric. The kernel X of the action of G on Γ_ρ must be contained in $K = N \cdot K(\alpha)$. But N is a minimal normal subgroup of G which acts non-trivially on the p ρ-classes involved in $(N_0)_1$; hence $N \cap X = 1$. Thus $N \times N \lhd K$ so X is a 2-group, normal in K. Since all K-orbits have length p^s it follows that $X = 1$. Hence G acts faithfully on Γ_ρ. However, N does not act semi-regularly on ρ-classes—for example, since N_0 leaves invariant each ρ-class in Δ_0. It follows from [2, Theorem 2.1] that $\Gamma_\rho = C(p; t, s-2)$, where $p^t \geq |N| = p^s$ so $t \geq s$; it follows from the structure of Γ that t must be a multiple of r. We show that $t = r$.

Each ρ-class can be labelled with an $(s-1)$-tuple $(x_1, \ldots, x_{s-2})_j \in (Z_p)^{s-2} \times Z_t$, where Δ_i is the union of all the ρ-classes the labels $(x_1, \ldots, x_{s-2})_j$ of which have subscript $j \equiv i \pmod r$. Let Δ_i^i denote the set of all vertices in Δ_i the ρ-class of which has label with subscript *equal to* i. Let N^i denote the setwise stabilizer of Δ_i^i in N. Then N^0 stabilizes Δ_0^0 and Δ_1, and hence leaves invariant the set of ρ-classes in Δ_1 which are joined to ρ-classes in Δ_0^0; that is, N^0 stabilizes the set of ρ-classes the labels of which have subscript equal to 1. Hence $N^0 = N^1$ is normalized by $\langle N, G(\alpha_0), \sigma\rangle = G$, so $N^0 = N$. Hence $t = r$. □

Lemma 5.2 suggests one possible strategy for identifying the graph Γ. First use $\Gamma_\rho = C(p; r, s-2)$ to label the ρ-classes in Γ, each of size p^2, in some convenient way; then use the groups $N_i = (Z_p)^2$ to provide each vertex of Γ with two additional co-ordinates, so that vertices of Γ correspond precisely to the labelling set $(Z_p)^s \times Z_r$ with adjacency determined by some simple rule (such as that for $C^{\pm 1}(p; r, s)$ or for $C^{\pm \varepsilon}(p; 2st, s)$). Implementing this strategy is less straightforward. In the extremal case studied in Section 7 it turns out to be simpler to use a direct approach. In general we see no obvious alternative to trying to exploit Lemma 5.2.

DEFINITION 5.3. A *cyclic t-arc* in Γ (or in Γ_ρ) is a sequence $(\beta_0, \beta_1, \ldots, \beta_t)$ of $t+1$ vertices such that each β_i $(0 \leq i \leq t)$ is adjacent to β_{i+1}, and β_{i-1} and β_{i+1} always lie in different N-orbits $(0 < i < t)$.

LEMMA 5.4. *We may label ρ-classes with elements of* $(Z_p)^{s-2} \times Z_r$ *in such a way that* $\rho(\alpha_i)$ *receives the label* $(0, 0, \ldots, 0)_i$ *for each* i $(0 \leq i < r)$.

PROOF. We use the automorphism group of $C(p; r, s-2)$ (*not* the automorphism group of Γ, which may be too small).

By [2], each orbit of N on ρ-classes corresponds to the set of all vertices $(x_1, \ldots, x_{s-2})_i$ of $C(p; r, s-2)$ with fixed subscript $i \in Z_r$. Since $\sigma: (x_1, \ldots, x_{s-2})_i \to (x_1, \ldots, x_{s-2})_{i+1}$ is an automorphism of $C(p; r, s-2)$, we can ensure that each ρ-class in Δ_0 corresponds to a vertex in $C(p; r, s-2)$ the label of which has the subscript $0 \in Z_r$. Since $\tau: (x_1, \ldots, x_{s-2})_i \to (x_{s-2}, \ldots, x_1)_{-i}$ is an automorphism of $C(p; r, s-2)$, we can then ensure that, for each $i \in Z_r$, each ρ-class in Δ_i corresponds to a vertex in $C(p; r, s-2)$ the label of which has the subscript i. Since $\operatorname{Aut} C(p; r, s-2) \geq S_p \operatorname{wr} D_{2r}$ we may use a suitable element from the base group $(S_p)^r$ to ensure that the ρ-class containing α_0 receives the label $(0, 0, \ldots, 0)_0$.

In Γ_ρ, $(\rho(\alpha_0), \rho(\alpha_1), \ldots, \rho(\alpha_{r-s+2}))$ is a cyclic $(r-s+2)$-arc; in $C(p; r, s-2)$, $(\mathbf{0}_0, \mathbf{0}_1, \ldots, \mathbf{0}_{r-s+2})$ is a cyclic $(r-s+2)$-arc. Since $\operatorname{Aut} C(p; r, s-2) \geq S_p \operatorname{wr} D_{2r}$ acts transitively on cyclic $(r-(s-2))$-arcs, we can ensure that the isomorphism $\varphi: \Gamma_\rho \to C(p; r, s-2)$, which is guaranteed by Lemma 5.2, labels the ρ-classes $\rho(\alpha_0), \rho(\alpha_1), \ldots, \rho(\alpha_{r-s+2})$ in the required way.

Suppose that $\varphi(\rho(\alpha_j)) \neq \mathbf{0}_j$ for some first j, $r-s+2 < j \leq r-1$. Since $\rho(\alpha_j)$ is adjacent to $\rho(\alpha_{j-1})$ in Γ_ρ, and since $\varphi(\rho(\alpha_{j-1})) = \mathbf{0}_{j-1}$, we must have $\varphi(\rho(\alpha_j)) = (0, \ldots, 0, x)_j$ for some $x \neq 0$. Now $(\varphi(\rho(\alpha_j)), \varphi(\rho(\alpha_{j+1})), \ldots, \varphi(\rho(\alpha_0)))$ is a cyclic $(r-j)$-arc in $C(p; r, s-2)$, so $\varphi(\rho(\alpha_{j+1})) = (0, \ldots, 0, x, y)_{j+1}$ for some $y \in Z_p$, $\varphi(\rho(\alpha_{j+2})) = (0, \ldots, 0, x, y, z)_{j+2}$ for some $z \in Z_p$, and so on. Since $r-j < s-2$, the non-zero co-ordinate x would then have to appear in the label for $\rho(\alpha_0)$, a contradiction. Hence $\varphi(\rho(\alpha_j)) = \mathbf{0}_j$ for each j. □

6. THE GENERAL CASE $N_i = (Z_p)^2$

Lemma 4.2 shows that the subgroup of N which leaves invariant each ρ-class in Δ_i is just $N_i = \langle a(i-1), a(i) \rangle$. Theorem 4.3 showed that if N_i has order p, then $\Gamma = C^{\pm 1}(p; r, 1)$ or $\Gamma = C^{\pm\varepsilon}(p; 2t, 1)$. This section concentrates on the general case in which each N_i has order p^2.

LEMMA 6.1. *For each* $i \in Z_r$ *we have*

$$N = \langle a(i-1) \rangle \times \langle a(i) \rangle \times \cdots \times \langle a(i+s-2) \rangle = N_i N_{i+1} \cdots N_{i+s-2}.$$

PROOF. By Lemma 5.2, $r \geq s$. If $r = s$, then the result is clearly true. So assume that $r > s$. Fix $i \in Z_r$, and for each $j \geq 2$ let $L_j = N_i N_{i+1} \cdots N_{i+j-2} = \langle a(i-1), a(i), \ldots, a(i+j-2) \rangle$. Since L_j is a subgroup of N and is generated by j elements, we have $|L_j| \leq p^j$; moreover, $|L_{j+1}| \leq p \cdot |L_j|$. Also, $|L_r| = |N| = p^s$, so $|L_r| < p^r$. Hence not all of $L_2, L_3, \ldots, L_{s+2}$ can be different: let k be the first subscript for which $L_k = L_{k+1}$. Then $|L_k| = p \cdot |L_{k-1}| = p^2 \cdot |L_{k-2}| = \cdots = p^{k-2} \cdot |L_2| = p^k$. We show that $L_k = N$, whence $k = s$ and the lemma follows.

Since $a(i-1)^\sigma = a(i)$, $0 < i < r-1$, and $a(r-1)^\sigma = a(0)$ or $a(0)^{-1}$, we have $N_j^\sigma = N_{j+1}$ for each $j \in Z_r$. Since $L_k = L_{k+1}$, we have $N_{i+k-1} \leq L_{k+1} = L_k =$

$N_iN_{i+1}\cdots N_{i+k-2}$. Thus $N_{i+k}=N^{\sigma}_{i+k-1}\leqslant N^{\sigma}_iN^{\sigma}_{i+1}\cdots N^{\sigma}_{i+k-2}=N_{i+1}N_{i+2}\cdots N_{i+k-1}$ $\leqslant N_iN_{i+1}\cdots N_{i+k-2}=L_k$; hence $L_{k+2}=L_k$. Continuing in this way we see that $L_k=L_{k+1}=\cdots=L_r=N_0N_1\cdots N_r$. But $N_0N_1\cdots N_r$ is a normal subgroup of G (since each N_i is precisely that subgroup of N which leaves each ρ-class in Δ_i invariant, and G merely permutes the sets Δ_i—and hence the subgroups N_i). Hence $L_k=L_r=N$ (by the minimality of N), so L_k has order p^s whence $k=s$. □

LEMMA 6.2. (a) *The group G acts regularly on the set of cyclic s'-arcs in Γ, where* $|K(\alpha_0)|=2^{s'}$.

(b) *The group* $K(\alpha_0)=\langle w(0),w(1),\ldots,w(s'-1)\rangle$, *where* $w(i)$ $(0\leqslant i<s')$ *centralizes $a(j)$ when $i+1\leqslant j\leqslant i+s'-1$ and inverts both $a(i)$ and $a(i+s')$. $K(\alpha_0)$ is elementary abelian of order $2^{s'}\leqslant 2^s$.*

PROOF. (a) Since Γ is G-symmetric, G acts transitively on the set of cyclic 1-arcs in Γ. Since $G(\alpha_0)$ is finite, there is a unique $s'\geqslant 1$ such that G acts transitively on cyclic s'-arcs, but not on cyclic $(s'+1)$-arcs. We show that G acts regularly on cyclic s'-arcs.

Let $(\beta_0,\beta_1,\ldots,\beta_{s'})$ by a cyclic s'-arc with $\beta_i\in\Delta_i$, and let $H=G(\beta_0\beta_1\cdots\beta_{s'})$ be its stabilizer in G. Then H not only fixes $\beta_0,\beta_1,\ldots,\beta_{s'}$, but must also fix pointwise both $\Gamma(\beta_{s'})\cap\Delta_{s'+1}$ and $\Gamma(\beta_0)\cap\Delta_{r-1}$. By shunting the cyclic s'-arc backwards and forwards we see that H must fix pointwise the whole connected component of Γ containing β_0. Hence $H=1$ (since Γ is connected), so G acts regularly on cyclic s'-arcs of Γ.

Since α_0 is the initial vertex of $4.2^{s'-1}$ cyclic s'-arcs, we have $|G(\alpha_0)|=4.2^{s'-1}=2^{s'+1}$; $|G(\alpha_0)\colon K(\alpha_0)|=2$ then implies $|K(\alpha_0)|=2^{s'}$.

(b) Let $(\alpha_i,\beta_{i+1},\ldots,\beta_{i+s'})$ be a cyclic s'-arc in Γ with $\beta_j\in\Delta_j$ $(i<j\leqslant i+s')$. The stabilizer of the $(s'-1)$-arc $(\alpha_i,\beta_{i+1},\ldots,\beta_{i+s'-1})$ is a subgroup $\langle w(i-1)\rangle$ of $K(\alpha_i)=K(\alpha_0)$ of order 2. Since β_{i+1} is joined to α_i, we must have either $\beta_{i+1}=a(i)_{i+1}$ or $\beta_{i+1}=a(i)^{-1}_{i+1}$; thus $w(i-1)$ centralizes $a(i)$. Since $\beta_{i+1}=(a(i)^{\pm 1}a(i+1)^{\pm 1})_{i+2}$, $w(i-1)$ also centralizes $a(i+1)$. Continuing in this way we see that $w(i-1)$ centralizes $a(i),a(i+1),\ldots,a(i+s'-2)$. Now $w(i-1)$ must act non-trivially on both $\Gamma(\alpha_i)\cap\Delta_{i-1}$ and $\Gamma(\beta_{i+s'-1})\cap\Delta_{i+s'}$, and so must invert $a(i-1)$ and $a(i+s'-1)$. Thus for each $i\leqslant s'-1$, $\langle w(0),\ldots,w(i-1)\rangle$ is a subgroup of $K(\alpha_0)$ which centralizes $a(i)$; since $w(i)$ inverts $a(i)$, we have $w(i)\notin\langle w(0),\ldots,w(i-1)\rangle$ $(0<i\leqslant s'-1)$. Hence $\langle w(0),\ldots,w(s'-1)\rangle$ has order at least $2^{s'}$, so $\langle w(0),\ldots,w(s'-1)\rangle=K(\alpha_0)$.

Now $K(\alpha_0)=K(\alpha_i)$ leaves $\Gamma(\alpha_i)\cap\Delta_{i+1}$ invariant, so elements of $K(\alpha_0)$ either centralize or invert $a(i)$. Thus the centralizer of $a(i)$ in $K(\alpha_0)$ has index at most 2. Hence the centralizer of $N=\langle a(0),a(1),\ldots,a(s-1)\rangle$ in $K(\alpha_0)$ has index at most 2^s. But $C_{K(\alpha_0)}(N)=1$ by Lemma 3.1(c), so $|K(\alpha_0)|=2^{s'}\leqslant 2^s$.

Finally, we show that $K(\alpha_0)$ is elementary abelian. The group G acts faithfully on $\Gamma_\rho=C(p;r,s-2)$ with $r\geqslant s$ (Lemma 5.2(b)). Since p is odd [2, Theorem 1.13] shows that either (i) $(r,s)=(4,1)$ with $\Gamma_\rho=K_{2p,2p}$ and $G\leqslant\operatorname{Aut}\Gamma_\rho=S_{2p}\operatorname{wr}S_2$, or (ii) $G\leqslant\operatorname{Aut}\Gamma_\rho=S_p\operatorname{wr}D_{2r}$. In case (i), $|K(\alpha_0)|=2^{s'}\leqslant 2^s=2$, so $K(\alpha_0)$ is certainly elementary abelian. In case (ii), $N=O_p(G)\neq 1$, so $G\leqslant L\operatorname{wr}D_{2r}$, where $L=Z_p\cdot Z_{p-1}$ is the holomorph of Z_p; hence $K\leqslant(L)^r$ and $K(\alpha_0)\leqslant(Z_{p-1})^r$, so $K(\alpha_0)$ is abelian, and thus elementary abelian (since it is generated by the involutions $w(0),\ldots,w(s'-1)$). □

It would seem that s' can indeed take any value between 1 and s. In general, we know that $a(0),a(0)^\sigma=a(1),\ldots,a(s-2)^\sigma=a(s-1)$ generate the group N of order p^s; all we know *a priori* about the element $a(s)=a(s-1)^\sigma$ is that it is equal to some linear combination of these generators (which must involve $a(0)$). When $s'=s$ it is relatively easy to pin down the possibilities for $a(s)$ (Section 7). When $s' < s$, the number of possibilities increases and the general picture becomes unclear. However, Lemma 6.2(b) implies that some things appear to be more restricted when $s' < s$ (see Section 8, where we examine the case $s = 2$ in detail and find that $C^{\pm\varepsilon}(p; 4t, 2)$ cannot occur).

7. The Extremal Case $s' = s$

In this section we restrict our attention to the case $s' = s$; that is, to the case in which $K(\alpha_0)$ is as large as it can possibly be. If we define elements $w(i-1)$, $i > 0$, as in (the proof of) Lemma 6.2(b), then the action of $K(\alpha_0) = \langle w(0), \ldots, w(s-1)\rangle$ is completely determined. We use this to pin down $a(s)$ precisely and to identify the possible graphs Γ.

Lemma 7.1. *Suppose that G acts regularly on cyclic s-arcs of Γ. Then*:
(a) *each $w(i)$ $(0 \leqslant i \leqslant s-1)$ centralizes $a(0), \ldots, a(i-1), a(i+1), \ldots, a(s-1)$ and inverts $a(i)$; also $w(i)^\sigma = w(i+1)$;*
(b) *$\langle a(i)\rangle = \langle a(i+s)\rangle$ for each $i \in Z_r$, so $r = st$ for some $t \geqslant 1$;*
(c) *$w(i+s-1)^\sigma = w(i+s) = w(i)$ for each $i \in Z_r$.*

Proof. $w(i)$ is defined to be the involution stabilizing some cyclic $(s-1)$-arc $(\alpha_{i+1}, \beta_{i+2}, \ldots, \beta_{i+s})$, where $\beta_j \in \Delta_j$. As in the proof of Lemma 6.2, $w(i)$ inverts $a(i)$ and $a(i+s)$ and centralizes $a(i+1), \ldots, a(i+s-1)$. Thus $w(i)$ stabilizes *every* cyclic s-arc of the form $(\alpha_{i+1}, \beta'_{i+2}, \ldots, \beta'_{i+s})$, where $\beta'_j \in \Delta_j$. Since σ maps the set of these cyclic s-arcs to those of the form $(\alpha_{i+2}, \beta''_{i+3}, \ldots, \beta''_{i+s+1})$ with $\beta''_j \in \Delta_j$, we must have $w(i)^\sigma = w(i+1)$. The fact that $w(i)$ centralizes $a(0), a(1), \ldots, a(i-1)$ then follows from the fact that $\langle a(j)\rangle = \langle a(j+s)\rangle$ (see next paragraph).

(b) We know that $a(s) \in N = \langle a(0), a(1), \ldots, a(s-1)\rangle$. Since $w(0)$ centralizes $a(1), \ldots, a(s-1)$ and inverts both $a(0)$ and $a(s)$, we must have $\langle a(0)\rangle = \langle a(s)\rangle$. Conjugating by σ^i yields $\langle a(i)\rangle = \langle a(i+s)\rangle$ for every $i \in Z_r$. In particular, $r \equiv 0 \pmod{s}$.

(c) The elements $w(i)$ and $w(i+s)$ both belong to $K(\alpha_0)$ and act in the same way on N, so $w(i)w(i+s)$ centralizes N. Hence, by Lemma 3.1(c), $w(i) = w(i+s)$. □

Lemma 7.1(b) shows that we must have $a(s) = a(0)^v$ for some $v \not\equiv 0 \pmod{p}$. The next result shows that there are essentially just two possibilities for v, and identifies Γ in each case.

Theorem 7.2. *Suppose that G acts regularly on s-arcs and that $a(s) = a(0)^v$. Then the elements σ and τ can be chosen so that either*
(a) *$v = \pm 1$, $\sigma^\tau = \sigma^{-1}$ and $\Gamma = C^{\pm 1}(p; st, s)$ for some $t \geqslant 1$, or*
(b) *$v = \pm\varepsilon$, where $p \equiv 1 \pmod{4}$ and $\varepsilon^2 \equiv -1 \pmod{p}$, $\sigma^\tau = w(0)\sigma^{-1}$, and $\Gamma = C^{\pm\varepsilon}(p; 2st, s)$ for some $t \geqslant 1$.*

Proof. G contains a unique element τ which maps the s-arc

$$(\alpha_0^{a(0)\cdots a(i-1)}\alpha_1^{a(1)\cdots a(i-1)} \ldots \alpha_{i-1}^{a(i-1)}\alpha_i\alpha_{i+1}^{a(i)} \ldots \alpha_s^{a(s-1)\cdots a(i)}),$$

where $s = 2i$ or $2i+1$, to the s-arc

$$(\alpha_s^{a(s-1)\cdots a(s-i)}\alpha_{s-1}^{a(s-2)\cdots a(s-i)} \ldots \alpha_{s-i+1}^{a(s-i)}\alpha_{s-i}\alpha_{s-i-1}^{a(s-i-1)} \ldots \alpha_0^{a(0)\cdots a(s-i-1)}).$$

Thus τ maps α_i to α_{s-i}, normalizes $K(\alpha_i) = K(\alpha_{s-i})$ and so (by Lemma 3.2) acts by conjugation on N taking $a(j)$ to $a(s-j-1)$ $(0 \leqslant j \leqslant s-1)$. Hence τ maps α_j to α_{s-j}

for each j, $0 \leq j \leq s-1$, and so maps the second s-arc back to the first; thus $\tau^2 = 1$ (since G acts regularly on s-arcs).

It is easy to check that $(\tau\sigma)^2 \in K(\alpha_i)$ and that $(\tau\sigma)^2$ centralizes $a(1), a(2), \ldots, a(s-1)$: and since $a(s) = a(0)^v$, $(\tau\sigma)^2$ conjugates $a(0)$ to $a(0)^{v^2}$. But elements of $K(\alpha_i) = \langle w(0), \ldots, w(s-1) \rangle$ can only centralize or invert $a(0)$, so $v^2 = \pm 1$.

(a) Suppose that $v^2 = +1$. Then $v = \pm 1$ and $(\tau\sigma)^2 \in C_{K(\alpha_0)}(N) = 1$, so $\sigma^\tau = \sigma^{-1}$. We now use the decomposition $N = \langle a(0) \rangle \times \cdots \times \langle a(s-1) \rangle$ to assign a label $(x_0, x_1, \ldots, x_{s-1})_i \in (Z_p)^s \times Z_r$ to each vertex in Δ_i. If $\beta \in \Delta_i$ is the image of α_i under $n = a(0)^{x_0} a(1)^{x_1} \cdots a(s-1)^{x_{s-1}}$, then we label β with the ordered $(s+1)$-tuple $(x_0, x_1, \ldots, x_{s-1})_i$. Thus α_i, with label $(0, \ldots, 0, 0, 0, \ldots, 0)_i$, is adjacent to $\alpha_{i+1}^{a(i)}$, with label $(0, \ldots, 0, 1, 0, \ldots, 0)_{i+1}$, and to $\alpha_{i+1}^{a(i)^{-1}}$, with label $(0, \ldots, 0, -1, 0, \ldots, 0)_{i+1}$, where the non-zero entry in each case occurs in the ith co-ordinate position. Since every edge in Γ is the image of such an edge under N, we have precisely $\Gamma = C^{\pm 1}(p; st, s)$ (see Definition 2.2).

(b) Suppose that $v^2 = -1$. Then $p \equiv 1 \pmod 4$ and $v = \pm\varepsilon$, where $\varepsilon^2 \equiv -1 \pmod p$. Moreover, $1 \neq (\tau\sigma)^2 \in C_{K(\alpha_0)}(\langle a(1), a(2), \ldots, a(s-1) \rangle) = \langle w(0) \rangle$, so $\sigma^\tau = w(0)\sigma^{-1}$. We now use the decomposition $N = \langle a(0) \rangle \times \cdots \times \langle a(s-1) \rangle$ exactly as in part (a) to assign a label $(x_0, x_1, \ldots, x_{s-1})_i \in (Z_p)^s \times Z_r$ to each vertex in Δ_i. This time the adjacency rules are visibly those for $C^{\pm\varepsilon}(p; 2st, s)$ (see Definition 2.3). □

This completes the proof of Theorem 1.1.

8. The Case $s = 2$

Since Γ is G-symmetric and $|G(\alpha_0): K(\alpha_0)| = 2$, we know in general that $2^s \geq |K(\alpha_0)| = 2^{s'} \geq 2$. When $s = 1$, the assumption $s = s'$ is therefore automatically satisfied. To gain some insight into what can happen when $|K(\alpha_0)| = 2^{s'} < 2^s$ it seems worth examining the case $s = 2$ in some detail (although this case is to some extent degenerate, in that the distance 2 graph Δ_i' induced on each component has just one component, so that $\Gamma_p = \Gamma_N = C_r = C(p; r, 0)$).

We shall assume throughout this section that $s = 2$: that is, that $N = \langle a(i-1) \rangle \times \langle a(i) \rangle = N_i = (Z_p)^2$ for each $i \in Z_r$. Hence $K(\alpha_0) = Z_2$ or $(Z_2)^2$ by Lemma 6.2. If $K(\alpha_0) = (Z_2)^2$, then Γ is determined by Theorem 7.2. Thus *we shall assume further that* $K(\alpha_0) = \langle w(0) \rangle = Z_2$. Hence G acts regularly on 1-arcs, and $G(\alpha_0) = (Z_2)^2$ or Z_4. Moreover, since $K(\alpha_0) = K(\alpha_1)$, we have $w(0)^\sigma = w(1)$.

Since G acts regularly on 1-arcs, the element σ which maps the 1-arc $(\alpha_0, \alpha_1^{a(0)})$ to the 1-arc $(\alpha_1, \alpha_2^{a(1)})$, and which conjugates each $a(i)$ to $a(i+1)$ $(0 \leq i < r-1)$ is uniquely determined. Now $a(1)^\sigma = a(2) \in N = \langle a(0), a(1) \rangle$, so $a(1)^\sigma = a(0)^m a(1)^k$ for some m and k. Clearly, $m \not\equiv 0 \pmod p$, since σ does not normalize $\langle a(1) \rangle$. The group G also contains a unique element τ which maps the 1-arc $(\alpha_1, \alpha_0^{a(0)})$ to the 1-arc $(\alpha_1, \alpha_2^{a(1)})$. Thus τ conjugates $a(0)$ to $a(1)$. Also, τ must map $\Gamma(\alpha_1) \cap \Delta_2$ to $\Gamma(\alpha_1) \cap \Delta_0$; so either τ conjugates $a(1)$ to $a(0)$, in which case $\tau^2 = 1$ and $G(\alpha_1) = \langle w(0), \tau \rangle = (Z_2)^2$, or τ conjugates $a(1)$ to $a(0)^{-1}$, in which case $\tau^2 = w(0)$ and $G(\alpha_1) = \langle \tau \rangle = Z_4$.

One would like to identify all possible pairs m, k and the corresponding graphs Γ. We achieve this only implicitly: ideally, one would like to know much more about the graphs Γ which occur in Lemmas 8.4 and 8.7.

Lemma 8.1. *Suppose that* $a(1)^\sigma = a(2) = a(0)^m a(1)^k$. *Then* $m \not\equiv 0 \pmod p$ *and one of the following holds.*

(1) $a(1)^\tau = a(0)$, $G(\alpha_1) = \langle \tau, w(0) \rangle = (Z_2)^2$, $\sigma^\tau = \sigma^{-1}$ *and*:

(1.1) $a(1)^\sigma = a(2) = a(0)$; *or*
(1.2) $a(1)^\sigma = a(2) = a(0)^{-1}$; *or*
(1.3) $a(1)^\sigma = a(2) = a(0)^{-1}a(1)^k$, *where* $k \not\equiv 0 \pmod p$.
(2) $a(1)^\tau = a(0)^{-1}$, $\tau^2 = w(0)$, $G(\alpha_1) = \langle\tau\rangle = Z_4$, $\sigma^\tau = \tau^2\sigma^{-1}$ *and*:
(2.1) $a(1)^\sigma = a(2) = a(0)$; *or*
(2.2) $a(1)^\sigma = a(2) = a(0)^{-1}$; *or*
(2.3) $a(1)^\sigma = a(2) = a(0)a(1)^k$, *where* $k \not\equiv 0 \pmod p$.

PROOF. The group $\langle\sigma, \tau\rangle$ induces D_{2r} on the circuit Γ_N. Hence $(\tau\sigma)^2 \in K$. Since $\alpha_1^{(\tau\sigma)^2} = \alpha_1$, we have $(\tau\sigma)^2 \in K(\alpha_1) = \langle w(0)\rangle$. Moreover, $a(1)^\tau = a(0)^{\pm 1}$, so $a(1)^{(\tau\sigma)^2} = a(1)$, whereas $w(0) = w(1)$ inverts $a(1)$. Hence $(\tau\sigma)^2 = 1$. Let $a(1)^\sigma = a(0)^m a(1)^k$.

(1) Suppose that $a(1)^\tau = a(0)$. Then $\tau^2 = 1$, so $(\tau\sigma)^2 = 1$ implies $\sigma^\tau = \sigma^{-1}$, and $G(\alpha_1) = \langle\tau, w(0)\rangle = (Z_2)^2$. Now $a(0) = a(0)^{(\tau\sigma)^2} = a(1)^{\sigma\tau\sigma} = (a(0)^m a(1)^k)^{\tau\sigma} = (a(1)^m a(0)^k)^\sigma = a(0)^{m^2} a(1)^{k(m+1)}$. Hence $m^2 \equiv 1 \pmod p$ and $k(m+1) \equiv 0 \pmod p$, so we have one of

(1.1) $m = 1$, $k = 1$, or (1.2) $m = -1$, $k = 0$, or (1.3) $m = -1$, $k \neq 0$.

(2) Suppose that $a(1)^\tau = a(0)^{-1}$. Then $\tau^2 = w(0)$, $G(\alpha_1) = \langle\tau\rangle = Z_4$ and $\sigma^\tau = \tau^2 \cdot \sigma^{-1}$. As before, $a(0) = a(0)^{(\tau\sigma)^2} = a(1)^{\sigma\tau\sigma} = (a(0)^m a(1)^k)^{\tau\sigma} = (a(1)^m a(0)^{-k})^\sigma = a(0)^{m^2} a(1)^{k(m-1)}$. Hence $m^2 \equiv 1 \pmod p$ and $k(m-1) \equiv 0 \pmod p$, so we have one of

(2.1) $m = 1$, $k = 0$, or (2.2) $m = -1$, $k = 0$, or (2.3) $m = 1$, $k \neq 0$.

□

We now consider each of these six possibilities (1.1), (1.2), (1.3), (2.1), (2.2) and (2.3) in turn.

LEMMA 8.2. *Suppose* (1.1): $a(1)^\tau = a(0)$, $a(1)^\sigma = a(0)$, $\sigma^\tau = \sigma^{-1}$ *and* $G(\alpha_1) = \langle\tau, w(0)\rangle = (Z_2)^2$. *Then* $r = 2t$ *is even,* $\sigma^r = 1$, $\Gamma = C^{\pm 1}(p; 2t, 2)$ *and* $\langle a(0)a(1)\rangle \lhd G$, *so N is not a minimal normal subgroup.*

PROOF. $\Gamma(\alpha_i) \cap \Delta_{i+1} = \{a(0)_{i+1}, a(0)_{i+1}^{-1}\}$ or $\{a(1)_{i+1}, a(1)_{i+1}^{-1}\}$ according as i is even or odd. Hence $r = 2t$ must be even. Then $\sigma^r \in K(\alpha_0)$ centralizes N, so $\sigma^r = 1$. Since $w(0)$ inverts both $a(0)$ and $a(1)$ (by Lemma 6.2) we have $\langle a(0)a(1)\rangle \lhd N\langle w(0), \sigma, \tau\rangle = G$, so N is not a minimal normal subgroup. Nevertheless, if we label vertices as in Theorem 7.2, we obtain $\Gamma = C^{\pm 1}(p; 2t, 2)$. □

LEMMA 8.3. *Suppose* (1.2): $a(1)^\tau = a(0)$, $a(1)^\sigma = a(0)^{-1}$, $\sigma^\tau = \sigma^{-1}$ *and* $G(\alpha_1) = \langle\tau, w(0)\rangle = (Z_2)^2$. *Then* $r = 2t$ *is even. If* $r \equiv 2 \pmod 4$, *then* $\sigma^r = w(0)$; *if* $r \equiv 0 \pmod 4$, *then* $\sigma^r = 1$. *In either case* $\Gamma = C^{\pm 1}(p; 2t, 2)$.

PROOF. The proof is similar to that of Lemma 8.2. □

LEMMA 8.4. *Suppose* (1.3): $a(1)^\tau = a(0)$, $a(1)^\sigma = a(0)^{-1}a(1)^k$ *with* $k \neq 0$, $\sigma^\tau = \sigma^{-1}$ *and* $G(\alpha_1) = (Z_2)^2$. *Then* $\sigma^r \in \langle w(0)\rangle$ *and r must be divisible by the first n for which*

$$\begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix}^n = \pm I.$$

PROOF. The element σ induces an automorphism of $N=(Z_p)^2$ which has matrix

$$\begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix}$$

relative to the basis $a(0)$, $a(1)$. Clearly, $\sigma^r \in K(\alpha_1)=\langle w(0)\rangle$, so σ^r has matrix I (if $\sigma^r=1$) or $-I$ (if $\sigma^r=w(0)$). □

LEMMA 8.5. *Suppose* (2.1): $a(1)^\tau=a(0)^{-1}$, $a(1)^\sigma=a(0)$, $\sigma^\tau=\tau^2\sigma^{-1}$, $\tau^2=w(0)$ *and* $G(\alpha_1)=Z_4$. *Then* $r=2t$ *is even,* $\sigma^r=1$ *and* $\Gamma=C^{\pm 1}(p;2t,2)$.

PROOF. The proof is similar to that of Lemma 8.2. □

LEMMA 8.6. *Suppose* (2.2): $a(1)^\tau=a(0)^{-1}$, $a(1)^\sigma=a(0)^{-1}$, $\sigma^\tau=\tau^2\sigma^{-1}$, $\tau^2=w(0)$ *and* $G(\alpha_1)=Z_4$. *Then* $r=2t$ *is even. If* $r\equiv 2 \pmod 4$, *then* $\sigma^r=w(0)$; *if* $r\equiv 0 \pmod 4$, *then* $\sigma^r=1$. *In either case* $\Gamma=C^{\pm 1}(p;2t,2)$ *and* N *is minimal normal only if* $p\equiv 3 \pmod 4$.

PROOF. If $p\equiv 1 \pmod 4$, then $p=u^2+v^2$ for some integers u and v. The group $\langle a(0)^u a(1)^v\rangle=Z_p$ is then normalized by $\langle N, w(0), \tau, \sigma\rangle=G$. The rest is similar to the proof of Lemma 8.2. □

LEMMA 8.7. *Suppose* (2.3): $a(1)^\tau=a(0)^{-1}$, $a(1)^\sigma=a(0)a(1)^k$ *with* $k\neq 0$, $\sigma^\tau=\tau^2\sigma^{-1}$, $\tau^2=w(0)$ *and* $G(\alpha_1)=Z_4$. *Then* $r=2t$, $\sigma^r\in\langle w(0)\rangle$, *and r must be divisible by the first (necessarily even) n such that*

$$\begin{pmatrix} 0 & 1 \\ 1 & k \end{pmatrix}^n=\pm I.$$

PROOF. The proof is similar to that of Lemma 8.4. □

Thus, when $s=2$ and $|K(\alpha)|=2^{s'}<2^s$, we obtain the graphs $\Gamma=C^{\pm 1}(p;2t,2)$ which occurred in Section 7, together with the graphs in Lemmas 8.4 and 8.7. It would be interesting to have a purely combinatorial description of these latter graphs. For different values of k, the matrix

$$\begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix}$$

In Lemma 8.4 would seem to generate all possible cyclic subgroups of $SL(2,p)$: for example, $k=1$ generates Z_3; $k=-1$ generates Z_6; $k=\pm 2$ generates Z_p; $k=\pm 3$ generate Z_M and Z_{2M}, where $2M$ is the first even suffix for which F_{2M}—the $2M$th Fibonacci number—is divisible by p (the precise value of M is an old unsolved problem, although it is known that M divides $(p+1)/2$ if $p\equiv\pm 2 \pmod 5$ and that M divides $(p-1)/2$ if $p\equiv\pm 1 \pmod 5$); and so on. Similarly, the matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & k \end{pmatrix}$$

in Lemma 8.7 with different values of k would seem to generate all even order cyclic subgroups of $SL(2,p)$.

Acknowledgements

The first author wishes to thank the University of Western Australia for its hospitality while this work was being done. The work was partially supported by ARC grant A68830358.

References

1. A Gardiner and C. E. Praeger, On 4-valent symmetric graphs, *Europ. J. Combin.* **15** (1994), 375–381.
2. C. E. Praeger and M.-Y. Xu, A characterization of a class of symmetric graphs of twice prime valency, *Europ. J. Combin.*, **10** (1989), 91–102.

Received 19 December 1991 and accepted in revised form 28 October 1993

A. Gardiner
School of Mathematics and Statistics,
University of Birmingham,
Birmingham B15 2TT, U.K.

Cheryl E. Praeger
Department of Mathematics,
University of Western Australia,
Nedlands, Western Australia 6009